ABSTRACT

Numerous formal approaches to software assurance are available, including runtime monitoring, model-checking, and theorem proving. All these approaches require formal specifications of behavioral properties to verify a software system. Creation of formal specifications is difficult, and previously, there has been inadequate tool support for this task. The Property Specification tool, Prospec, was developed to assist users in the creation of formal specifications. This work describes Prospec 2.0, an improvement to the previous version, by addressing the results of a study conducted to assess the usability of the tool and by adding functionality that supports the validation process.

MOTIVATION

- The effectiveness of the assurance approach depends on the quality of the formal specifications.
- A significant hurdle to the use of formal approaches is the creation of correct formal specifications.
- Typically, the person creating the formal specification must:
  - Have a strong mathematical background
  - Be aware of the subtleties and differences in expressiveness of the specification language
- The Property Specification (Prospec) 1.0 was developed to address some of these challenges.

BACKGROUND

- Prospec 1.0:
  - Allows users to formalize software properties based on high-level requirements.
  - Specifies program properties using scopes and patterns as defined by the Specification Format System’s (SFS) and Compositional Propositions (CP)
  - Generates formalized specifications in the following languages:
    - Future Interval Logic (FIL)
    - Meta-Event Definition Language (MEDL)
    - Linear Temporal Logic (LTL)
  - A formal expression of the effects that Prospec and SFS have over the quality of the generated software properties with respect to completeness and correctness
  - The following research hypothesis was supported: users who specify software properties using Prospec correctly identify, on average, more patterns and scopes than users who specify software properties using the SFS web site.
  - The subjects provided comments for improving Prospec, which are addressed through Prospec 2.0

PROSPEC 2.0 NEW FEATURES

- Prospec 2.0 includes new features to support the specification of properties.
- The interface maintains the support and functionality of the original Prospec.
- The main changes are related primarily to information presentation.

SUMMARY

This work describes Prospec 2.0, an improvement to the property specification tool Prospec 1.0. The new features enable practitioners to use Prospec 2.0 as an automated formal property specification tool and as an automated formal property validation tool. The major improvements in Prospec 2.0 are related to information presentation. A Property Browsing view provides users quick access to add, delete, and modify properties and propositions. A Property Summary view summarizes the completeness status of the property or proposition being specified.

REFERENCES